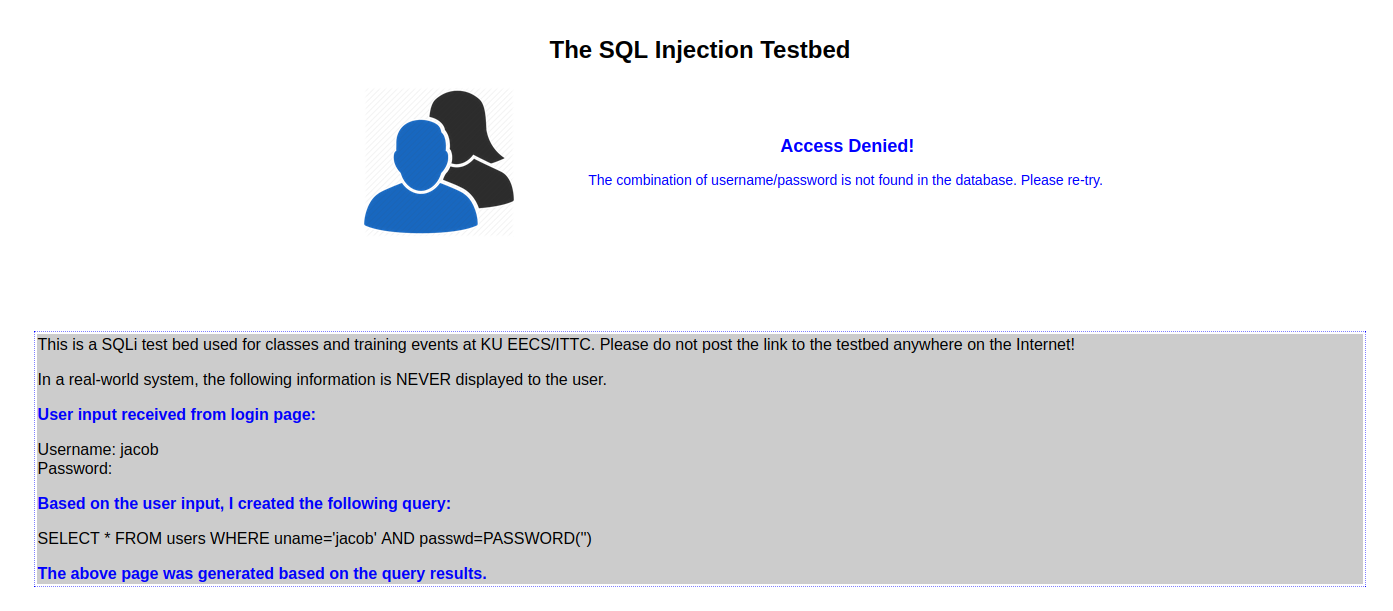
Mini-Project 4

**Task 1: You are asked to try SQL Injection attacks on a testbed:**[**https://cae.ittc.ku.edu/sqli/login.html**](https://cae.ittc.ku.edu/sqli/login.html)**. Please compose malicious input to exploit this vulnerable web application and achieve the following attack goals. Login as any user without providing the password. That is, you know the username, say "jacob", but you do NOT know Jacob's password. Login as Jacob.**

1. I have entered “**jacob**” in the username box only and used the Login button without providing the password. Then, the testbed shows me that the access is denied since the password box is empty. The inputs and the results are shown on these screenshots of this task.

**Screenshots:**

A computer screen shot of a person pointing

Description automatically generated

**Task 2: Steal all records in the table: you do not know the username or password of any user. Find a way to display all the user profiles.**

1. I have found a way to display the users and their profiles of the database by applying the query logic, entering “**’ OR true #**” in the username box only, and using the Login button without providing the password. Then, the testbed shows me that the login is successful because it is displaying the users and their respective profiles. There are too many users to show in the report, but I have managed to take the screenshots of the top users and the last users. But you can display the users’ records by the query logic and the command that are used in this task. The inputs and the results are shown on these screenshots of this task.

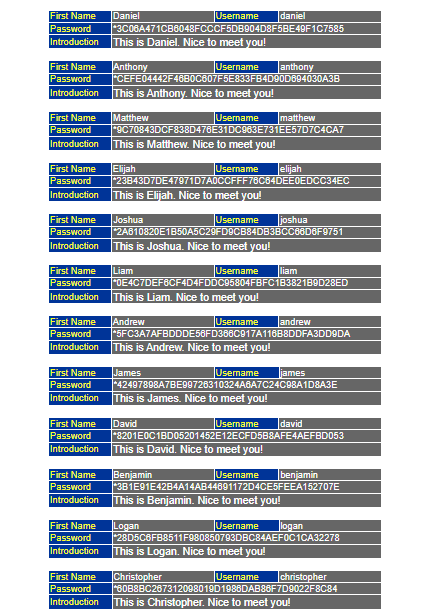
**Screenshots:**

A hand pointing to a login box

Description automatically generated A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer

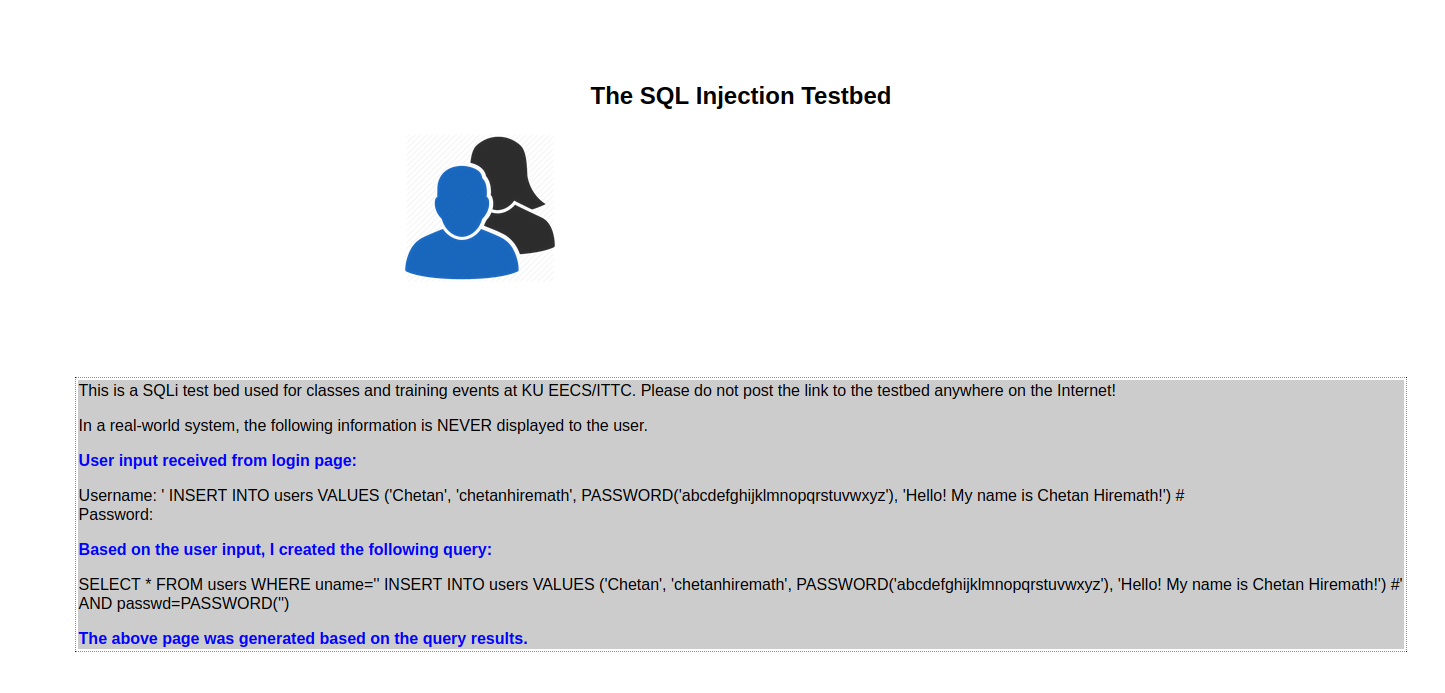
Description automatically generated

**Task 3: Insert a record (the platform now allows multiple queries concatenated by a semicolon), make sure that you include something about yourself (your name or nickname or screen name) in the new record -- just to tell the world that you have been there. Please also make sure that you can log in as this new user.**

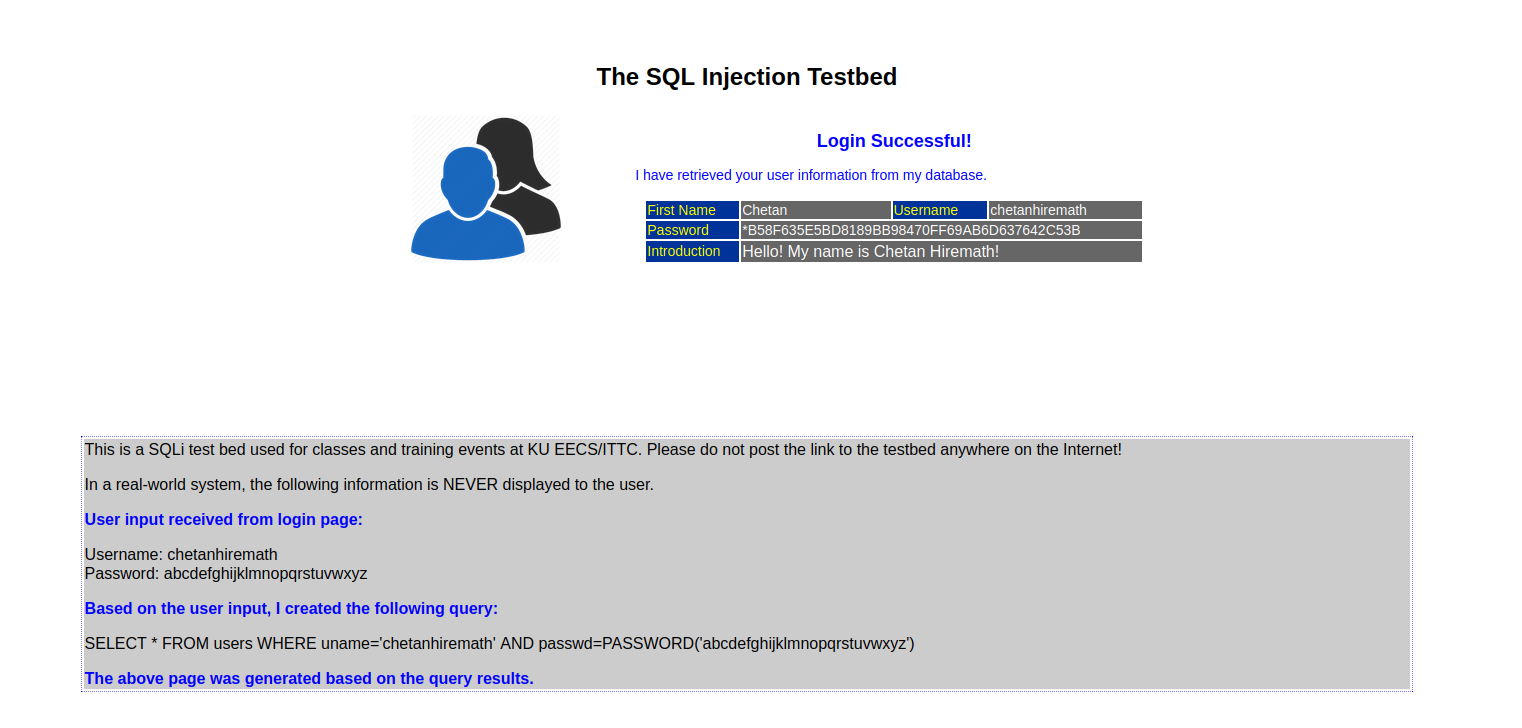
1. I have inserted a new record by applying the query logic, entering “**' INSERT INTO users VALUES ('Chetan', 'chetanhiremath', PASSWORD('abcdefghijklmnopqrstuvwxyz'), 'Hello! My name is Chetan Hiremath!') #**”in the username box only, and using the Login button without providing the password. Then, the testbed shows me nothing since the record is created and inserted in the database successfully. I have made sure that I can use the Login button as a new user, so I have entered “**chetanhiremath**” and “**abcdefghijklmnopqrstuvwxyz**” in the username and the password boxes respectively and used the Login button. Then, the testbed shows me that the login is successful because it is displaying my inserted record and its information. The inputs and the results are shown on these screenshots of this task.

**Screenshots:**

A screenshot of a login page

Description automatically generated 

A hand pointing to a login screen

Description automatically generated 

**Task 4: Try the above attacks in the safe web application at:**[**https://cae.ittc.ku.edu/sql/login.html**](https://cae.ittc.ku.edu/sql/login.html)**and report whether they can succeed.**

1. I have used the safe web application, which is similar to the testbed, to try the first 3 attacks/tasks and see whether they succeed or not. They don’t succeed because the safe web application is showing me that the special characters in the input string are escaped, so the input is secure for SQL. Also, I notice that there is a backslash (\) before the special character (‘) because “escaping” characters tell SQL values that the values are treated as strings only. The inputs and the results are shown on these screenshots of this task.

**Screenshots:**

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated

A screenshot of a login page

Description automatically generated A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated A screenshot of a computer

Description automatically generated